Entanglement-assisted quantum error-correcting codes over arbitrary finite fields

Galindo, Carlos; Hernando, Fernando; Yamashita, Ryutaro; Ruano, Diego

Published in:
Quantum Information Processing

DOI (link to publication from Publisher):
10.1007/s11128-019-2234-5

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

Quantum Information Processing (2019) 18:116
https://doi.org/10.1007/s11128-019-2234-5

Entanglement-assisted quantum error-correcting codes over arbitrary finite fields

Carlos Galindo[1] · **Fernando Hernando**[1] · **Ryutaroh Matsumoto**[2,3] · **Diego Ruano**[4]

Received: 11 December 2018 / Accepted: 25 February 2019 / Published online: 4 March 2019

Abstract
We prove that the known formulae for computing the optimal number of maximally entangled pairs required for entanglement-assisted quantum error-correcting codes (EAQECCs) over the binary field hold for codes over arbitrary finite fields as well. We also give a Gilbert–Varshamov bound for EAQECCs and constructions of EAQECCs coming from punctured self-orthogonal linear codes which are valid for any finite field.

Keywords Entanglement-assisted quantum error-correcting codes · Symplectic, Hermitian and Euclidean duality · Gilbert–Varshamov bound

Mathematics Subject Classification 81P70 · 94B65 · 94B05

Supported by the Spanish Ministry of Economy/FEDER: Grants MTM2015-65764-C3-1-P, MTM2015-65764-C3-2-P, MTM2015-69138-REDT and RYC-2016-20208 (AEI/FSE/UE), the University Jaume I: Grant UJI-B2018-10, Spanish Junta de CyL: Grant VA166G18, and JSPS Grant No. 17K06419.

✉ Diego Ruano
diego.ruano@uva.es

Carlos Galindo
galindo@uji.es

Fernando Hernando
carrillf@uji.es

Ryutaroh Matsumoto
ryutaroh.matsumoto@nagoya-u.jp

1 Departamento de Matemáticas, Instituto Universitario de Matemáticas y Aplicaciones de Castellón , Universitat Jaume I, Campus de Riu Sec, 12071 Castellón de la Plana, Spain

2 Department of Information and Communication Engineering, Nagoya University, 464-8603 Nagoya, Japan

3 Department of Mathematical Sciences, Aalborg University, 9220 Aalborg, Denmark

4 IMUVA-Mathematics Research Institute, University of Valladolid, 47011 Valladolid, Spain

1 Introduction

The Shor's proposal of using quantum error correction for reducing decoherence in quantum computation [24] and his polynomial-time algorithms for prime factorization and discrete logarithms on quantum computers [25] clearly illustrate the feasibility and importance of quantum computation and quantum error correction.

Most of the quantum error-correcting codes (QECCs) come from classical codes. The first known stabilizer quantum codes were binary [5,10]. Later, stabilizer codes over any finite field were introduced and studied and they are of particular interest because of their utility in fault-tolerant computation. Following [13], one can obtain QECCs of length n over a finite field $\mathbb{F}_q$ from additive codes included in $\mathbb{F}_q^{2n}$ which are self-orthogonal with respect to a trace-symplectic form. Working on this construction, QECCs of length n over $\mathbb{F}_q$ can be derived from classical self-orthogonal codes with respect to the Hermitian inner product included in $\mathbb{F}_{q^2}^n$ and also from codes in $\mathbb{F}_q^n$ which are self-orthogonal with respect to the Euclidean inner product.

The previously mentioned self-orthogonality conditions (or some similar requirements of inclusion of codes in the dual of others) prevent the usage of many common classical codes for providing quantum codes. Brun et al. [3] proposed to share entanglement between encoder and decoder to simplify the theory of quantum error correction and increase the communication capacity. With this new formalism, entanglement-assisted quantum stabilizer codes can be constructed from any classical linear code giving rise to entanglement-assisted quantum error-correcting codes (EAQECCs). A formula to obtain the optimal number of ebits required for a binary entanglement-assisted code of Calderbank–Shor–Steane (CSS) type was shown in [12], and formulae for more general constructions, including the consideration of duality with respect to symplectic forms, were given in [26]. In fact, [26] proves that the optimal number c of ebits required for a binary entanglement-assisted quantum error-correcting code with generator matrix $(H_X|H_Z)$ is $\operatorname{rank}(H_X H_Z^T - H_Z H_X^T)/2$, where the superindex T means transpose. Remark 1 in that paper states, without a proof, that the same formula holds when considering codes over finite fields $\mathbb{F}_p$, p being a prime number; a proof can be found in [18].

Recently, one can find in the literature some papers where the above formula (or formulae derived from it) is used for determining the entanglement corresponding to EAQECCs over arbitrary finite fields (see, for instance, [6,9,17,21]). Although it holds for any finite field, we have found no proof in the literature and, thus, this work fills this gap. Therefore, this paper is devoted to prove formulae for the minimum required number c of pairs of maximally entangled quantum states, corresponding to EAQECCs codes obtained from linear codes C over any finite field, by using symplectic forms, or Hermitian or Euclidean inner products. We also show (see Sect. 2.4) that in the Hermitian and Euclidean cases, c is easy to compute when one chooses, as a basis of the linear code C of length n, a subset of those vectors giving rise to a geometric decomposition of the coordinate space of dimension n that contains C [22].

In [15], a Gilbert–Varshamov-type formula for the existence of binary EAQECCs was presented. Still with the idea of extending the binary case to the general one and with the help of our study of entanglement-assisted codes, we give a Gilbert–

Varshamov-type formula which is valid for any finite field. Furthermore, we will also provide conditions of existence and parameters of EAQECCs coming from classical self-orthogonal codes (say C) over any finite field. Since fewer qudits should be transmitted through a noisy channel, they perform better. Constructions of this type have been considered in the binary case for giving a coding scheme with imperfect ebits [15].

Theorems 1, 3 and 4 contain our results about the entanglement required for EAQECCs over arbitrary finite fields. Section 2 also explains how, in the Hermitian and Euclidean cases, nice bases of the vector spaces that contain the supporting linear codes allow us to get the corresponding required number c. Section 3 is devoted to state the mentioned Gilbert–Varshamov-type bound, and Sect. 4 contains our results about EAQECCs coming from QECC by considering symplectic, Hermitian or Euclidean duality.

2 EAQECCs over $\mathbb{F}_q$

The first three subsections of this section are devoted to prove formulae for computing the optimal entanglement corresponding to EAQECCs over arbitrary finite fields when considering symplectic forms, or Hermitian or Euclidean inner products.

2.1 The symplectic case

Let p be a prime number and q a positive power $q = p^m$. Denote by $\mathbb{F}_q$ the finite field with q elements. We also write $\mathbb{C}$ the field of complex numbers and $\mathbb{C}^r$, r a positive integer, the r-coordinate space over $\mathbb{C}$.

Let n be a positive integer, it is known (see, for instance, [13, Theorem 13]) that an $((n, K, d))_q$ stabilizer quantum code over $\mathbb{F}_q$ can be obtained from an additive code $C \subseteq \mathbb{F}_q^{2n}$ of size q^n/K such that $C \subseteq C^{\perp_{ts}}$, and $\mathrm{swt}(C^{\perp_{ts}} \backslash C) = d$ when $K \geq 1$ and $d = \mathrm{swt}(C)$ otherwise. In the above result, we have considered the following notation which will be used in this paper as well. The symbol $\perp_{ts}$ means dual with respect to the *trace-symplectic form* on $\mathbb{F}_q^{2n}$:

$$(\mathbf{a}|\mathbf{b}) \cdot_{ts} \left(\mathbf{a}'|\mathbf{b}'\right) = \mathrm{tr}_{q/p}\left(\mathbf{a}\cdot\mathbf{b}' - \mathbf{a}'\cdot\mathbf{b}\right) \in \mathbb{F}_p,$$

where $(\mathbf{a}|\mathbf{b})$, $\left(\mathbf{a}'|\mathbf{b}'\right) \in \mathbb{F}_q^{2n}$, $\mathbf{a}\cdot\mathbf{b}'$ and $\mathbf{a}'\cdot\mathbf{b}$ are Euclidean products, and $\mathrm{tr}_{q/p} : \mathbb{F}_q \to \mathbb{F}_p$,

$$\mathrm{tr}_{q/p}(x) = x + x^p + \cdots + x^{p^{m-1}},$$

is the standard trace map. Also the symplectic weight is defined as

$$\mathrm{swt}\,(\mathbf{a}|\mathbf{b}) = \mathrm{card}\,\{i \mid (a_i, b_i) \neq (0,0), 1 \leq i \leq n\},$$

where $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)$.

We will also use the symplectic form on $\mathbb{F}_q^{2n}$ defined as

$$(\mathbf{a}|\mathbf{b}) \cdot_s \left(\mathbf{a}'|\mathbf{b}'\right) = \left(\mathbf{a}\cdot\mathbf{b}' - \mathbf{a}'\cdot\mathbf{b}\right) \in \mathbb{F}_q,$$

and the corresponding dual space for an $\mathbb{F}_q$-linear code $C \subseteq \mathbb{F}_q^{2n}$ will be denoted by $C^{\perp_s}$.

For the first part of this paper, we fix a trace orthogonal basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, $B = \{\gamma_1, \gamma_2, \ldots, \gamma_m\}$. Recall that B is a basis of $\mathbb{F}_q$ as a $\mathbb{F}_p$-linear space satisfying that the matrix

$$M = \left(\mathrm{tr}_{q/p}(\gamma_i\gamma_j)\right)_{1\leq i\leq m;\ 1\leq j\leq m}$$

is an invertible and diagonal matrix of size m with coefficients in $\mathbb{F}_p$. The existence of a basis as B is proved in [23]. We choose a basis as B by convenience, but our results also hold if one considers any other basis. Now consider the $\mathbb{F}_p$-linear map

$$h : \mathbb{F}_p^m \to \mathbb{F}_q, \quad h(x_1, x_2, \ldots, x_m) = \sum_{i=1}^{m} x_i\gamma_i := x.$$

The map h is an isomorphism of $\mathbb{F}_p$-linear spaces, and for $x \in \mathbb{F}_q$, $h^{-1}(x)$ gives the coordinates of x in the basis B.

Denote by Ω the inverse matrix of M, and Ω is a size m diagonal invertible matrix with entries in $\mathbb{F}_p$. Let $\omega_1, \omega_2, \ldots, \omega_m$ be its diagonal, and define the map:

$$\phi : \mathbb{F}_p^{2m} = \mathbb{F}_p^m \times \mathbb{F}_p^m \longrightarrow \mathbb{F}_q^2,$$

given by

$$\begin{aligned}\phi\left((x_1, x_2, \ldots, x_m)|(y_1, y_2, \ldots, y_m)\right) &= \left(\sum_{i=1}^{m} x_i\gamma_i, \sum_{i=1}^{m} y_i\omega_i\gamma_i\right)\\ &= \left(h(x_1, x_2, \ldots, x_m), h[(y_1, y_2, \ldots, y_m)\Omega]\right).\end{aligned}$$

Taking into account that $\omega_i \in \mathbb{F}_p$, $B' = \{\omega_i\gamma_i\}_{i=1}^m$ is also a trace orthogonal basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ whose matrix $\left(\mathrm{tr}_{q/p}(\omega_i\gamma_i\omega_j\gamma_j)\right)_{1\leq i\leq m;\ 1\leq j\leq m}$ is Ω.

In sum, ϕ is an isomorphism of $\mathbb{F}_p$-linear spaces and for $(x, y) \in \mathbb{F}_q^2$,

$$\phi^{-1}(x, y) = \left(\phi_1^{-1}(x, y), \phi_2^{-1}(x, y)\right) \in \mathbb{F}_p^{2m},$$

where ϕ_1^{-1} (respectively, ϕ_2^{-1}) is the first (respectively, second) projection of ϕ^{-1} over the first (respectively, second) component of the Cartesian product $\mathbb{F}_p^m \times \mathbb{F}_p^m$. One has that $\phi^{-1}(x, y)$ simply gives a pair whose first components are the coordinates of x in the basis B and the second ones are those of y in the basis B'.

The above map can be extended to products of n copies giving rise to the map

$$\phi^E : \mathbb{F}_p^{2mn} = (\mathbb{F}_p^m)^n \times (\mathbb{F}_p^m)^n \longrightarrow \mathbb{F}_q^n \times \mathbb{F}_q^n = \mathbb{F}_q^{2n},$$

defined by

$$\begin{aligned}&\phi^E\left[((a_{11},\ldots,a_{1m}),\ldots,(a_{n1},\ldots,a_{nm})|(b_{11},\ldots,b_{1m}),\ldots,(b_{n1},\ldots,b_{nm}))\right]\\&= (h(a_{11},\ldots,a_{1m}),\ldots,h(a_{n1},\ldots,a_{nm})|h[(b_{11},\ldots,b_{1m})\Omega],\ldots,h[(b_{n1},\ldots,b_{nm})\Omega])\,.\end{aligned}$$

Notice that ϕ^E is again an isomorphism of $\mathbb{F}_p$-linear spaces and

$$\left(\phi^E\right)^{-1}(\mathbf{a}|\mathbf{b}) = \left(\left(\phi^E\right)_1^{-1}(\mathbf{a}|\mathbf{b}) \mid \left(\phi^E\right)_2^{-1}(\mathbf{a}|\mathbf{b})\right),$$

where $\left(\phi^E\right)_1^{-1}$ (respectively, $\left(\phi^E\right)_2^{-1}$) is the first (respectively, second) projection of $\left(\phi^E\right)_1^{-1}$ over the first (respectively, second) component of the Cartesian product $(\mathbb{F}_p^m)^n \times (\mathbb{F}_p^m)^n$. One has that $\left(\phi^E\right)^{-1}(\mathbf{a}|\mathbf{b})$ equals the vector of coordinates of the element $(\mathbf{a}|\mathbf{b}) \in \mathbb{F}_q^{2n}$ in the basis of $\mathbb{F}_q^{2n}$ over $\mathbb{F}_p$ given by $\oplus_{n \text{ times}} B \bigoplus \oplus_{n \text{ times}} B'$.

Keeping the above notation, it is easy to deduce the following result in [2].

Proposition 1 *The following statements hold:*

a) Let $x, y \in \mathbb{F}_q$, then

$$\mathrm{tr}_{q/p}(xy) = \left(\phi_1^{-1}(x,y)\right) \cdot \left(\phi_2^{-1}(x,y)\right),$$

where $\cdot$ denotes the Euclidean product in $\mathbb{F}_p^m$.

b) Let $(\mathbf{a}|\mathbf{b}), \left(\mathbf{a}'|\mathbf{b}'\right) \in \mathbb{F}_q^{2n}$, then

$$\begin{aligned}&(\mathbf{a}|\mathbf{b}) \cdot_{st} \left(\mathbf{a}'|\mathbf{b}'\right)\\&= \left[\left(\phi^E\right)_1^{-1}(\mathbf{a}|\mathbf{b}) \mid \left(\phi^E\right)_2^{-1}(\mathbf{a}|\mathbf{b})\right] \cdot_s \left[\left(\phi^E\right)_1^{-1}\left(\mathbf{a}'|\mathbf{b}'\right) \mid \left(\phi^E\right)_2^{-1}\left(\mathbf{a}'|\mathbf{b}'\right)\right],\end{aligned}$$

where $\cdot_s$ denotes the symplectic form in $\mathbb{F}_p^{2mn}$.

Our purpose in this section is to determine the optimal required number of pairs of maximally entangled states of the EAQECC over an arbitrary finite field $\mathbb{F}_q$ that can be constructed from an $\mathbb{F}_q$-linear code $C \subseteq \mathbb{F}_q^{2n}$ with dimension $n-k$. Assume that $(H_X|H_Z)$ is an $(n-k) \times 2n$ generator matrix of C. The case when $m = 1$ (i.e., q is prime) is known (see [18,26]), and the corresponding result is the following:

Theorem 1 *Let $C \subseteq \mathbb{F}_p^{2n}$ be an $(n-k)$-dimensional $\mathbb{F}_p$-linear space and $H = (H_X|H_Z)$ an $(n-k) \times 2n$ matrix whose row space is C. Let $C' \subseteq \mathbb{F}_p^{2(n+c)}$ be an*

$\mathbb{F}_p$-linear space such that the projection of C' to the $1, 2, \ldots, n, n+c+1, n+c+2, \ldots, 2n+c$-th coordinates is equal to C and $C' \subseteq (C')^{\perp_s}$, where c is the minimum required number of maximally entangled quantum states in $\mathbb{C}^p \otimes \mathbb{C}^p$. Then,

$$2c = \operatorname{rank}\left(H_X H_Z^T - H_Z H_X^T\right).$$

The encoding quantum circuit is constructed from C', and it encodes $k+c$ logical qudits in $\mathbb{C}^p \otimes \cdots (k+c \text{ times}) \cdots \otimes \mathbb{C}^p$ into n physical qudits using c maximally entangled pairs. The minimum distance is $d := d_s\left(C^{\perp_s} \backslash (C \cap C^{\perp_s})\right)$, where

$$d_s\left(C^{\perp_s} \backslash (C \cap C^{\perp_s})\right) = \min\left\{\operatorname{swt}(\mathbf{a}|\mathbf{b}) \mid (\mathbf{a}|\mathbf{b}) \in C^{\perp_s} \backslash (C \cap C^{\perp_s})\right\}.$$

In sum, C provides an $[[n, k+c, d; c]]_p$ EAQECC over the field $\mathbb{F}_p$.

Theorem 1 states that the required number of maximally entangled quantum states is given by the rank of the matrix $H_X H_Z^T - H_Z H_X^T$. Our next result shows that even in the case of codes over an arbitrary finite field $\mathbb{F}_q$, the above number depends only on the code C and its symplectic dual.

Proposition 2 *Let $C \subseteq \mathbb{F}_q^{2n}$ be a linear code over $\mathbb{F}_q$ and $(H_X|H_Z)$ its $(n-k) \times 2n$ generator matrix. Then,*

$$\operatorname{rank}\left(H_X H_Z^T - H_Z H_X^T\right) = \dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q}(C \cap C^{\perp_s}).$$

Proof Consider the $\mathbb{F}_q$-linear map $f : \mathbb{F}_q^{2n} \to \mathbb{F}_q^{n-k}$ defined by $f(\mathbf{a}|\mathbf{b}) = \mathbf{a}H_Z^T - \mathbf{b}H_X^T$. Set $\operatorname{row}(H_X|H_Z)$ the row space of the matrix $(H_X|H_Z)$. Then, we have

$$\begin{aligned}\operatorname{rank}\left(H_X H_Z^T - H_Z H_X^T\right) &= \dim_{\mathbb{F}_q} f(\operatorname{row}(H_X|H_Z)) \\ &= \dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q} C \cap \ker(f) \\ &= \dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q}(C \cap C^{\perp_s}),\end{aligned}$$

which concludes the proof. □

Next, with the help of the above proposition, we prove that Theorem 1 can be extended to codes over any finite field $\mathbb{F}_q$.

Theorem 2 *Let $C \subseteq \mathbb{F}_q^{2n}$ be an $(n-k)$-dimensional $\mathbb{F}_q$-linear space and $H = (H_X|H_Z)$ a matrix whose row space is C. Let $C' \subseteq \mathbb{F}_q^{2(n+c)}$ be an $\mathbb{F}_q$-linear space such that its projection to the coordinates $1, 2, \ldots, n, n+c+1, n+c+2, \ldots, 2n+c$ equals C and $C' \subseteq (C')^{\perp_s}$, where c is the minimum required number of maximally entangled quantum states in $\mathbb{C}^q \otimes \mathbb{C}^q$. Then,*

$$2c = \operatorname{rank}\left(H_X H_Z^T - H_Z H_X^T\right) = \dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q}\left(C \cap C^{\perp_s}\right).$$

The encoding quantum circuit is constructed from C', and it encodes $k+c$ logical qudits in $\mathbb{C}^q \otimes \cdots (k+c \text{ times}) \cdots \otimes \mathbb{C}^q$ into n physical qudits using c maximally entangled pairs. The minimum distance is $d := d_s\left(C^{\perp_s} \backslash (C \cap C^{\perp_s})\right)$, where d_s is defined as in Theorem 1. In sum, C provides an $[[n, k+c, d; c]]_q$ EAQECC over the field $\mathbb{F}_q$.

Proof One has that the inclusion $C^{\perp_s} \subseteq C^{\perp_{ts}}$ holds since $\mathrm{tr}_{q/p}(0) = 0$. In addition, $C^{\perp_{ts}} \subseteq C^{\perp_s}$. Indeed, following [2], if $(\mathbf{a}|\mathbf{b}) \in C^{\perp_{ts}}$, then $(\mathbf{a}|\mathbf{b}) \cdot_{ts} (\mathbf{x}|\mathbf{y}) = 0$ for all $(\mathbf{x}|\mathbf{y}) \in C$. Taking into account that $\alpha\,(\mathbf{x}|\mathbf{y}) \in C$ for any $\alpha \in \mathbb{F}_q$, then $\mathrm{tr}_{q/p}\left((\mathbf{a}|\mathbf{b}) \cdot_s \alpha(\mathbf{x}|\mathbf{y})\right) = 0$ for all α. This means that $\mathrm{tr}_{q/p}\left(\alpha\left((\mathbf{a}|\mathbf{b}) \cdot_s (\mathbf{x}|\mathbf{y})\right)\right) = 0$ for all α, which proves $(\mathbf{a}|\mathbf{b}) \cdot_s (\mathbf{x}|\mathbf{y}) = 0$ and, therefore $(\mathbf{a}|\mathbf{b}) \in C^{\perp_s}$.

Now, using the same notation as at the beginning of this section, consider the code over the field $\mathbb{F}_p$, $C_0 := (\phi^E)^{-1}(C)$. It is clear that $\dim_{\mathbb{F}_p}(C_0) = m(n-k)$, and by Proposition 1 and the equality $C^{\perp_s} = C^{\perp_{ts}}$, we have

$$\dim_{\mathbb{F}_p} C_0 = m(n-k) = m \dim_{\mathbb{F}_q} C.$$

Thus,

$$\dim_{\mathbb{F}_p} C_0 - \dim_{\mathbb{F}_p} C_0 \cap C_0^{\perp_s} = m\left(\dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q}(C \cap C^{\perp_s})\right).$$

This shows that by Theorem 1, we have an entanglement-assisted quantum code encoding $m(k+c)$ qudits in $\mathbb{C}^p$ and consuming mc maximally entangled states in $\mathbb{C}^p \otimes \mathbb{C}^p$. Using the map ϕ^E and the fact that $C^{\perp_s} = C^{\perp_{ts}}$, we have an entanglement-assisted quantum code encoding $(k+c)$ qudits in $\mathbb{C}^q$ and consuming c maximally entangled states in $\mathbb{C}^q \otimes \mathbb{C}^q$. In fact, one can construct $C_0' \subseteq \mathbb{F}_p^{2m(n+c)}$ in the same way as constructed C' from C in Theorem 1. Applying ϕ^E to the code C_0', we get the code C' in the statement with the claimed properties. The minimum distance follows from [13, Section III]. □

2.2 The Hermitian case

In this subsection, we specialize the results in Sect. 2.1 by considering the Hermitian inner product instead of a symplectic form. With the above notation, consider the finite field $\mathbb{F}_{q^2}$ and a normal basis $\{w, w^q\}$ of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Fix a positive integer n and, following [13], define a trace-alternating form over $\mathbb{F}_{q^2}^n$ as

$$\mathbf{x} \cdot_a \mathbf{y} = \mathrm{tr}_{q/p}\left(\frac{\mathbf{x} \cdot \mathbf{y}^q - \mathbf{x}^q \cdot \mathbf{y}}{w^{2q} - w^2}\right),$$

where $\mathbf{z}^q, \mathbf{z} \in \mathbb{F}_{q^2}^n$, means the componentwise q-power of $\mathbf{z}$. The map $\varphi : \mathbb{F}_q^{2n} \to \mathbb{F}_{q^2}^n$ given by $\varphi\,(\mathbf{a}|\mathbf{b}) = w\mathbf{a} + w^q\mathbf{b}$ is bijective and isometric because the symplectic and the Hamming weights of $(\mathbf{a}|\mathbf{b})$ and $\varphi\,(\mathbf{a}|\mathbf{b})$ coincide. In addition, for $(\mathbf{a}|\mathbf{b})$, $\left(\mathbf{a}'|\mathbf{b}'\right) \in \mathbb{F}_q^{2n}$, it holds that

$$(\mathbf{a}|\mathbf{b}) \cdot_{ts} \left(\mathbf{a}'|\mathbf{b}'\right) = \varphi\,(\mathbf{a}|\mathbf{b}) \cdot_a \varphi\left(\mathbf{a}'|\mathbf{b}'\right).$$

Recall that the Hermitian inner product of two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_{q^2}^n$ is defined to be $\mathbf{x} \cdot_h \mathbf{y} = \mathbf{x}^q \cdot \mathbf{y}$, where $\cdot$ means Euclidean product, and that, in [13], it is proved that for a $\mathbb{F}_{q^2}$-linear code D, the dual codes with respect to the products $\cdot_a$ and $\cdot_h$ coincide. With the above ingredients, we are ready to prove the next proposition which will allow us to state and prove our theorem on EAQECCs over arbitrary finite fields by considering Hermitian inner product.

Proposition 3 *Let $C \subseteq \mathbb{F}_{q^2}^n$ be a code over $\mathbb{F}_{q^2}$ of dimension $(n-k)/2$ for some positive integer k. Let H be its generator matrix. Then,*

$$\operatorname{rank}(HH^*) = \dim_{\mathbb{F}_{q^2}} C - \dim_{\mathbb{F}_{q^2}} (C \cap C^{\perp_h}),$$

where H^* is the qth power of the transpose matrix of H.

Proof Define the $\mathbb{F}_{q^2}$-linear map $f : \mathbb{F}_{q^2}^n \to \mathbb{F}_{q^2}^{(n-k)/2}$, given by $f(\mathbf{a}) = \mathbf{a}H^*$. Then,

$$\begin{aligned} \operatorname{rank}(HH^*) &= \dim_{\mathbb{F}_{q^2}} f(\operatorname{row}(H)) \\ &= \dim_{\mathbb{F}_{q^2}} C - \dim_{\mathbb{F}_{q^2}} (C \cap \ker(f)) \\ &= \dim_{\mathbb{F}_{q^2}} C - \dim_{\mathbb{F}_{q^2}} (C \cap C^{\perp_h}). \end{aligned}$$

□

Theorem 3 *Let $C \subseteq \mathbb{F}_{q^2}^n$ be an $(n-k)/2$-dimensional code over $\mathbb{F}_{q^2}$, for suitable integers n and k. Denote by H its generator matrix. Let $C' \subseteq \mathbb{F}_{q^2}^{(n+c)}$ be an $\mathbb{F}_{q^2}$-linear space whose projection to the coordinates $1, 2, \ldots, n$ equals C and satisfies $C' \subseteq (C')^{\perp_h}$, where c is the minimum required number of maximally entangled quantum states in $\mathbb{C}^q \otimes \mathbb{C}^q$. Then,*

$$c = \operatorname{rank}\left(HH^*\right) = \dim_{\mathbb{F}_{q^2}} C - \dim_{\mathbb{F}_{q^2}} \left(C \cap C^{\perp_h}\right).$$

The encoding quantum circuit is constructed from C', and it encodes $k+c$ logical qudits in $\mathbb{C}^q \otimes \cdots (k+c \text{ times}) \cdots \otimes \mathbb{C}^q$ into n physical qudits using c maximally entangled pairs. The minimum distance is $d := d_H\left(C^{\perp_h} \backslash (C \cap C^{\perp_h})\right)$, where d_H is defined as the minimum Hamming weight of the vectors in the set $C^{\perp_h} \backslash \left(C \cap C^{\perp_h}\right)$. In sum, C provides an $[[n, k+c, d; c]]_q$ EAQECC over the field $\mathbb{F}_q$.

Proof With the above notation, consider the code C' in $\mathbb{F}_{q^2}^n$ of dimension $n-k$ whose generator matrix is

$$\mathcal{H} = \begin{pmatrix} \omega H \\ \omega^q H \end{pmatrix}$$

and set $C_0 = \varphi^{-1}(C')$ the corresponding code in $\mathbb{F}_q^{2n}$. Since φ is an isometry, to obtain the value $2c$ corresponding to C_0, it suffices to compute the rank of the matrix given

by the form $\cdot_a$ which is $\mathcal{J} = \mathrm{tr}_{q^2/q}\left((HH^* - H^q H^T)/\lambda\right)$, where $\lambda = \omega^{2q} - \omega^2$ and $\mathrm{tr}_{q^2/q}$ the trace map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. Now, setting

$$\mathcal{Z} = \begin{pmatrix} \omega^{q+1} & \omega^2 \\ \omega^{2q} & \omega^{q+1} \end{pmatrix},$$

it holds that $\mathcal{J} = (2/\lambda)\left(ZHH^* - Z^T H^q H^T\right)$. Performing elementary operations, we get that $\mathrm{rank}(\mathcal{J}) = 2\,\mathrm{rank}\,(HH^*)$. Finally, by our previous considerations, $\dim_{\mathbb{F}_q} C_0 = n - k$, $\dim_{\mathbb{F}_q}(C_0 \cap C_0^{\perp_s}) = 2c$, and

$$d_H\left(C^{\perp_h} \backslash C^{\perp_h} \cap C\right) = d_s\left(C_0^{\perp_s} \backslash (C^{\perp_s} \cap C_0)\right),$$

which proves our statement by Theorem 2. □

The following corollary is an immediate consequence of the above result.

Corollary 1 *Let C be an $[n, k, d]_{q^2}$ linear code over $\mathbb{F}_{q^2}$, and set H a parity check matrix of C. Then, there exists an $[[n, 2k - n + c, d; c]]_q$ EAQECC where $c = \mathrm{rank}(HH^*)$, H^* is the qth power of the transpose matrix H^T.*

2.3 The Euclidean case

In this section, we will show that EAQECCs over any finite field $\mathbb{F}_q$ can be obtained through a CSS construction, where the Euclidean inner product is considered, and carried out with two $\mathbb{F}_q$-linear codes C_1 and C_2 of length n. Assume that C_1 (respectively, C_2) has dimension k_1 and generator matrix H_1 (respectively, k_2 and H_2). Before stating our result, we give the following proposition which will be used in its proof.

Proposition 4 *With the above notations, it holds that*

$$\mathrm{rank}(H_1 H_2^T) = \dim_{\mathbb{F}_q} C_1 - \dim_{\mathbb{F}_q}(C_1 \cap C_2^{\perp}), \tag{1}$$

and

$$\mathrm{rank}(H_2 H_1^T) = \dim_{\mathbb{F}_q} C_2 - \dim_{\mathbb{F}_q}(C_2 \cap C_1^{\perp}), \tag{2}$$

where $\perp$ means Euclidean dual.

Proof To prove Equality (1), consider the $\mathbb{F}_q$-linear map $f : \mathbb{F}_q^n \to \mathbb{F}_q^{k_2}$ defined by the matrix H_2^T, that is $f(\mathbf{a}) = \mathbf{a}H_2^T$. Then,

$$\begin{aligned} \mathrm{rank}(H_1 H_2^T) &= \dim_{\mathbb{F}_q} f(\mathrm{row}(H_1)) \\ &= \dim_{\mathbb{F}_q} C_1 - \dim_{\mathbb{F}_q}(C_1 \cap \ker(f)) \\ &= \dim_{\mathbb{F}_q} C_1 - \dim_{\mathbb{F}_q}(C_1 \cap C_2^{\perp}). \end{aligned}$$

Equality (2) follows analogously from the map given by H_1^T. □

Next, we state the main result in this section.

Theorem 4 *Let C_1 and C_2 be two linear codes over $\mathbb{F}_q$ included in $\mathbb{F}_q^n$ with respective dimensions k_1 and k_2 and generator matrices H_1 and H_2. Then, the code $C_0 = C_1 \times C_2 \subseteq \mathbb{F}_q^{2n}$ gives rise to an EAQECC which encodes $n - k_1 - k_2 + c$ logical qudits into n physical qudits using the minimum required of maximally entangled pairs c, which is*

$$c = \operatorname{rank}(H_1 H_2^T) = \dim_{\mathbb{F}_q} C_1 - \dim_{\mathbb{F}_q}(C_1 \cap C_2^{\perp}).$$

The minimum distance of the entanglement-assisted quantum code is larger than or equal to

$$d := \min\left\{d_H\left(C_1^{\perp} \backslash (C_2 \cap C_1^{\perp})\right), d_H\left(C_2^{\perp} \backslash (C_1 \cap C_2^{\perp})\right)\right\}.$$

In sum, one gets an $[[n, n - k_1 - k_2 + c, d; c]]_q$ EAQECC.

Proof It suffices to notice that $\dim_{\mathbb{F}_q} C_0 = k_1 + k_2$, $C_0^{\perp_s} = C_2^{\perp} \times C_1^{\perp}$, and

$$\begin{aligned}
&\dim_{\mathbb{F}_q} C_0 - \dim_{\mathbb{F}_q}(C_0^{\perp_s} \cap C_0) \\
&= \dim_{\mathbb{F}_q}(C_1 \times C_2) - \dim_{\mathbb{F}_q}\left((C_2^{\perp} \cap C_1) \times (C_1^{\perp} \cap C_2)\right) \\
&= \left(\dim_{\mathbb{F}_q} C_1 - \dim_{\mathbb{F}_q}(C_2^{\perp} \cap C_1)\right) + \left(\dim_{\mathbb{F}_q} C_2 - \dim_{\mathbb{F}_q}(C_1^{\perp} \cap C_2)\right) \\
&= 2c.
\end{aligned}$$

By construction, we have that

$$d_s(C_0 \backslash C_0^{\perp_s}) \geq \min\left\{d_H\left(C_1^{\perp} \backslash (C_2 \cap C_1^{\perp})\right), d_H\left(C_2^{\perp} \backslash (C_1 \cap C_2^{\perp})\right)\right\},$$

and then our statement follows from Theorem 2. □

2.4 Geometric decomposition of the coordinate space

In this subsection, we consider only the Hermitian and Euclidean cases, and we will explain that the required number of maximally entangled pairs is easy to compute when the generators of the supporting $\mathbb{F}_q$-linear code C in $\mathbb{F}_q^n$ are a subset of a basis of $\mathbb{F}_q^n$ with a special metric structure which is said to be *compatible with a geometric decomposition* of $\mathbb{F}_q^n$ (see [22]). Notice that in the Hermitian case, q should be q^2; however, for simplicity's sake and only in this subsection, we will use q as a generic symbol which means a power of a prime in the Euclidean case or an even power of a prime in the Hermitian case. For avoiding to repeat notation, again only in this subsection, $\langle \mathbf{a}, \mathbf{b} \rangle$ will mean either the Hermitian inner product $\mathbf{a} \cdot_h \mathbf{b}$ or the Euclidean one $\mathbf{a} \cdot \mathbf{b}$.

Let us introduce some notation, we say that $\{\mathbf{v}_1, \mathbf{v}_2\}$ are *geometric generators of a hyperbolic plane* if $\langle \mathbf{v}_1, \mathbf{v}_1\rangle = \langle \mathbf{v}_2, \mathbf{v}_2\rangle = 0$ and $\langle \mathbf{v}_1, \mathbf{v}_2\rangle = 1$. We say that $\{\mathbf{v}_1, \mathbf{v}_2\}$ are *geometric generators of an elliptic plane* if $\langle \mathbf{v}_1, \mathbf{v}_1\rangle = 0$ and $\langle \mathbf{v}_2, \mathbf{v}_2\rangle = \langle \mathbf{v}_1, \mathbf{v}_2\rangle = 1$. Finally, we say that $\mathbf{v}$ *generates a non-singular space* if $\langle \mathbf{v}, \mathbf{v}\rangle \neq 0$.

Let $C \subseteq \mathbb{F}_q^n$ and set $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ a basis of $\mathbb{F}_q^n$ such that C is generated by $\{\mathbf{v}_i\}_{i\in I}$ for $I \subseteq \{1, 2, \ldots, n\}$. We say that C is *compatible with a geometric decomposition* of $\mathbb{F}_q^n$ if

$$\mathbb{F}_q^n = H_1 \oplus \cdots \oplus H_r \oplus L_1 \oplus \cdots \oplus L_s,$$

where the linear spaces from H_1, generated by $\{\mathbf{v}_1, \mathbf{v}_2\}$, to H_r, generated by $\{\mathbf{v}_{2r-1}, \mathbf{v}_r\}$, are hyperbolic planes, being the $\mathbf{v}_i$ geometric generators, and from L_1, generated by $\mathbf{v}_{2r+1}$, to L_s, generated by $\mathbf{v}_{2r+s} = \mathbf{v}_n$, are non-singular spaces. Then, we say that the vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r$ (and the indexes $1, 2, \ldots r$) are asymmetric and the vectors $\mathbf{v}_{r+1}, \mathbf{v}_{r+2}, \ldots, \mathbf{v}_n$ (and the indexes $r+1, r+2, \ldots, n$) are symmetric. Moreover, we also say that $(1, 2), \ldots, (r-1, r)$ are symmetric pairs.

In [22], for the Euclidean inner product, it was proved that for characteristic different from 2, we can always obtain a basis $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n\}$ of $\mathbb{F}_q^n$ such that

$$\mathbb{F}_q^n = H_1 \oplus \cdots \oplus H_r \oplus L_1 \oplus \cdots \oplus L_s,$$

with $s \leq 4$. For characteristic equal to 2, we may have a decomposition as in the case with characteristic different from 2, excepting when the vector $(1, 1, \ldots, 1)$ belongs to the *radical* (or *hull*) of C, $C \cap C^{\perp}$. In that particular case, it was given in [22] the following decomposition

$$\mathbb{F}_q^n = H_1 \oplus \cdots \oplus H_r \oplus L_1 \oplus \cdots \oplus L_s \oplus E,$$

with $s \leq 2$ and where E is an elliptic plane.

Let $M = (\langle \mathbf{v}_i, \mathbf{v}_j\rangle)_{1\leq i,j\leq n}$, one has that M has the form

$$M = \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 0 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & 1 & 0 & & & & \\ & & & & & g_1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & g_s & \end{pmatrix},$$

where $g_1, \ldots, g_s$ are nonzero, except for the case when the characteristic is 2 and $(1, 1, \ldots, 1)$ belongs to the radical of C; then, we have that M is equal to

$$M = \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 0 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & 1 & 0 & & & & \\ & & & & & g_1 & & & \\ & & & & & & g_s & & \\ & & & & & & & 0 & 1 \\ & & & & & & & 1 & 1 \end{pmatrix}.$$

Now, let $i \in \{1, 2, \ldots, n\}$. We define i' as

- $i + 1$ if $\mathbf{v}_i$ is the first generator of a hyperbolic plane H,
- $i - 1$ if $\mathbf{v}_i$ is the second generator of a hyperbolic plane H,
- i if $\mathbf{v}_i$ generates a one-dimensional linear space L,
- $i + 1$ if $\mathbf{v}_i$ is the first generator of an elliptic plane E.

Notice that we do not define i' when $\mathbf{v}_i$ is the second geometric generator of an elliptic plane, because in this case, $(1, 1, \ldots, 1)$ is not in the radical of C [22]. For $I \subseteq \{1, 2, \ldots, n\}$, we set $I' = \{i' : i \in I\}$ and $I^\perp = \{1, 2, \ldots, n\} \backslash I'$. In this way, we can compute the dual code $C^\perp$ of a linear code C generated by $\{\mathbf{v}_i\}_{i \in I}$ easily since it is generated by $\{\mathbf{v}_i\}_{i \in I^\perp}$. Moreover, it can also be used to construct QECCs using the CSS construction since $C \subseteq C^\perp$ if and only if $I \subseteq I^\perp$. These kinds of decomposition arise naturally (i.e., for the usual generators) in some families of evaluation codes as BCH codes, toric codes, J-affine variety codes, negacyclic codes, constacylic codes, etc., and the previous approach has been exploited for constructing stabilizer quantum codes, EAQECCs and LCD codes (see [7–9,14,17] for instance).

The above paragraphs allow us to give a practical procedure for computing the value c given in Theorem 3, for the Hermitian product, and in Theorem 4, for the Euclidean product ($C_1 = C_2 = C$). Assume that C is a code generated by $\{\mathbf{v}_i\}_{i \in I}$ compatible with a geometric decomposition of the corresponding coordinate space and write $I = I_R \sqcup I_L$ (i.e., $I = I_R \cup I_L$ and $I_R \cap I_L = \emptyset$), where the radical of C, $C \cap C^\perp$, $\perp$ meaning dual with respect to the inner product $\langle\ ,\ \rangle$, is generated by $\{\mathbf{v}_i\}_{i \in I_R}$. The radical of C can be easily computed in this case: Indeed, given $i \in I$, one has that $i \in I_R$ if it holds that $\mathbf{v}_i$ is the first generator of a hyperbolic plane H and $i + 1 \notin I$, $\mathbf{v}_i$ is the second generator of a hyperbolic plane H and $i - 1 \notin I$, or $\mathbf{v}_i$ is the first generator of an elliptic plane E. Otherwise, $i \in I_L$. An equivalent way to characterize I_R is the following: I_R consists of asymmetric indexes whose pair does not belong to I and I_L consists of symmetric indexes and pairs of asymmetric indexes that belong to I. Summarizing, one has that when one considers a suitable basis as above, then

$$\begin{aligned} c &= \dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q} \left(C \cap C^\perp \right) = \operatorname{card}(I) - \operatorname{card}(I \cap I^\perp) \\ &= \operatorname{card}(I) - \operatorname{card}(I_R) = \operatorname{card}(I_L). \end{aligned}$$

Note that we have an EAQECC with maximal entanglement when $I = I_L$, i.e., when $I_R = \emptyset$. This fact was used, for instance, in [9].

3 Gilbert–Varshamov-type sufficient condition of existence of entanglement-assisted codes

In this section, we give a Gilbert–Varshamov-type bound which is valid for EAQECCs over arbitrary finite fields. A similar bound was stated in [16] for the binary case.

Theorem 5 *Assume the existence of positive integers $n, k \leq n, \delta, c \leq (n-k)/2$ such that*

$$\frac{q^{n+k} - q^{n-k-2c}}{q^{2n}-1} \sum_{i=1}^{\delta-1} \binom{n}{i} (q^2-1)^i < 1. \tag{3}$$

Then, there exists an $\mathbb{F}_q$-linear code $C \subseteq \mathbb{F}_q^{2n}$ such that $\dim_{\mathbb{F}_q} C = n-k$, $d_s(C^{\perp_s} \backslash (C^{\perp_s} \cap C)) \geq \delta$ and $\dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q}(C^{\perp_s} \cap C) = 2c$.

Proof We will use a close argument to the proof of the Gilbert–Varshamov bound for stabilizer codes [4,13]. Let $\mathrm{Sp}(q,n)$ be the symplectic group over $\mathbb{F}_q^{2n}$ [11, Section 3] and $A(k,c)$ the set of $\mathbb{F}_q$-linear spaces $V \subseteq \mathbb{F}_q^{2n}$ such that $\dim_{\mathbb{F}_q} V = n-k$ and

$$\dim_{\mathbb{F}_q} V - \dim_{\mathbb{F}_q} \left(V^{\perp_s} \cap V \right) = 2c.$$

For $\mathbf{0} \neq \mathbf{e} \in \mathbb{F}_q^{2n}$, define

$$B(k,c,\mathbf{e}) = \left\{ V \in A(k,c) \mid \mathbf{e} \in V^{\perp_s} \backslash (V^{\perp_s} \cap V) \right\}.$$

Taking into account that the symplectic group acts transitively on $\mathbb{F}_q^{2n} \backslash \{\mathbf{0}\}$ [1,11], it holds that for nonzero $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{F}_q^{2n}$, there exists $M \in \mathrm{Sp}(q,n)$ such that $\mathbf{e}_1 M = \mathbf{e}_2$, and, for $V_1, V_2 \in A(k,c)$, there exists $M \in \mathrm{Sp}(q,n)$ such that $V_1 M = V_2$.

Therefore, for nonzero elements $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{F}_q^{2n}$ with $\mathbf{e}_1 M_1 = \mathbf{e}_2$ $(M_1 \in \mathrm{Sp}(q,n))$ and some fixed linear space $V_1 \in A(k,c)$, we have the following chain of equalities:

$$\begin{aligned}
&\mathrm{card}\,(B(k,c,\mathbf{e}_1)) \\
&\quad = \mathrm{card}\left(\{ V \in A(k,c) \mid \mathbf{e}_1 \in V^{\perp_s} \backslash (V^{\perp_s} \cap V) \} \right) \\
&\quad = \mathrm{card}\left(\{ V_1 M \mid \mathbf{e}_1 \in V^{\perp_s} M \backslash (V^{\perp_s} M \cap VM),\ M \in \mathrm{Sp}(q,n) \} \right) \\
&\quad = \mathrm{card}\left(\{ V_1 M M_1^{-1} \mid \mathbf{e}_1 \in V^{\perp_s} M M_1^{-1} \backslash (V^{\perp_s} M M_1^{-1} \cap V M M_1^{-1}),\ M \in \mathrm{Sp}(q,n) \} \right) \\
&\quad = \mathrm{card}\left(\{ V_1 M \mid \mathbf{e}_1 M_1 \in V^{\perp_s} M \backslash (V^{\perp_s} M \cap VM),\ M \in \mathrm{Sp}(q,n) \} \right)
\end{aligned}$$

$$= \operatorname{card}\left(\{V_1 M \mid \mathbf{e}_2 \in V^{\perp_s} M \backslash (V^{\perp_s} M \cap VM),\, M \in \mathrm{Sp}(q,n)\}\right)$$
$$= \operatorname{card}\left(\{V \in A(k,c) \mid \mathbf{e}_2 \in V^{\perp_s} \backslash (V^{\perp_s} \cap V)\}\right)$$
$$= \operatorname{card}\left(B(k,c,\mathbf{e}_2)\right).$$

For each $V \in A(k,c)$, the number of vectors $\mathbf{e}$ in $\mathbb{F}_q^{2n}$ such that $\mathbf{e} \in V^{\perp_s} \backslash (V^{\perp_s} \cap V)$ is

$$\operatorname{card}(V^{\perp_s}) - \operatorname{card}\left(V^{\perp_s} \cap V\right) = q^{n+k} - q^{n-k-2c}.$$

The number of pairs $(\mathbf{e}, V)$ such that $\mathbf{0} \neq \mathbf{e} \in V^{\perp_s} \backslash (V^{\perp_s} \cap V)$ is

$$\sum_{\mathbf{0} \neq \mathbf{e} \in \mathbb{F}_q^{2n}} \operatorname{card}\left(B(k,c,\mathbf{e})\right) = \operatorname{card}\left(A(k,c)\right)\left(q^{n+k} - q^{n-k-2c}\right),$$

which implies

$$\frac{\operatorname{card}\left(B(k,c,\mathbf{e})\right)}{\operatorname{card}\left(A(k,c)\right)} = \frac{q^{n+k} - q^{n-k-2c}}{q^{2n}-1}. \tag{4}$$

If there exists $V \in A(k,c)$ such that $V \notin B(k,c,\mathbf{e})$ for all $1 \leq \mathrm{swt}(\mathbf{e}) \leq \delta - 1$, then there will exist V with the desired properties. The number of vectors $\mathbf{e}$ such that $1 \leq \mathrm{swt}(\mathbf{e}) \leq \delta - 1$ is given by

$$\sum_{i=1}^{\delta-1} \binom{n}{i} (q^2-1)^i. \tag{5}$$

By combining Equalities (4) and (5), we see that Inequality (3) is a sufficient condition for ensuring the existence of a code C as in our statement. This ends the proof. □

To finish this section, we derive an asymptotic form of Theorem 5.

Theorem 6 *Let R, ϵ and λ be nonnegative real numbers such that $R \leq 1$, $\epsilon < 1/2$ and $\lambda \leq (1-R)/2$. Let $h(x) := -x \log_q x - (1-x)\log_q(x-1)$ be the q-ary entropy function. For n sufficiently large, the inequality*

$$h(\epsilon) + \epsilon \log_q(q^2-1) < 1 - R, \tag{6}$$

implies the existence of a code $C \subseteq \mathbb{F}_q^{2n}$ over $\mathbb{F}_q$ such that

$$\dim_{\mathbb{F}_q} C = \lceil n(1-R) \rceil, \quad d_s(C^{\perp_s} \backslash (C^{\perp_s} \cap C)) \geq \lfloor n\epsilon \rfloor$$

and

$$\dim_{\mathbb{F}_q} C - \dim_{\mathbb{F}_q}(C^{\perp_s} \cap C) = \lfloor 2n\lambda \rfloor.$$

Proof It follows from Theorem 5 using a similar reasoning to that in [19, Section III.C]. □

4 EAQECCs coming from punctured QECCs

Our final section gives parameters of EAQECCs obtained from punctured codes coming from self-orthogonal codes with respect to symplectic forms, or Hermitian or Euclidean inner products. Since fewer qudits should be transmitted through a noisy channel, they perform better. Let us start with the symplectic case.

4.1 Symplectic form

Let $C \subseteq \mathbb{F}_q^{2n}$ be an $\mathbb{F}_q$-linear code. The *puncturing* of C to the coordinate set $\{1, \ldots, n-c\}$ is defined as the code of length $2(n-c)$ given by

$$P(C) = \big\{(a_1, \ldots, a_{n-c}|b_1, \ldots, b_{n-c}) \mid (a_1, \ldots, a_n|b_1, \ldots, b_n) \in C \\ \text{for some } a_{n-c+1}, \ldots, a_n, b_{n-c+1}, \ldots, b_n \in \mathbb{F}_q\big\}.$$

In addition, the *shortening* of C to the coordinate set $\{1, \ldots, n-c\}$ is defined as the code

$$S(C) = \{(a_1, \ldots, a_{n-c}|b_1, \ldots, b_{n-c}) \mid \\ (a_1, \ldots, a_{n-c}, 0, \ldots, 0|b_1, \ldots, b_{n-c}, 0, \ldots, 0) \in C\}.$$

When we have a stabilizer code given by an $\mathbb{F}_q$-linear code C such that $C \subseteq C^{\perp_s} \subseteq \mathbb{F}_q^{2n}$, we can construct an entanglement-assisted code from $P(C) \subseteq \mathbb{F}_q^{2(n-c)}$. By [20], $P(C)^{\perp_s} = S(C^{\perp_s})$ and we deduce

$$P(C) \cap P(C)^{\perp_s} = P(C) \cap S(C^{\perp_s}) = S(C \cap C^{\perp_s}) = S(C).$$

The minimum distance of the constructed entanglement-assisted code is $d_s(S(C^{\perp_s}) \setminus S(C))$ which is larger than or equal to $d_s(C^{\perp_s} \setminus C)$. Following [20], one can prove the following result.

Proposition 5 *Assume that a positive integer c satisfies $2c \leq d_H(C \setminus \{\mathbf{0}\}) - 1$, then*

$$\dim_{\mathbb{F}_q} P(C) = \dim_{\mathbb{F}_q} C, \quad \textit{and}$$

$$\dim_{\mathbb{F}_q} P(C) \cap P(C)^{\perp_s} = \dim_{\mathbb{F}_q} S(C) = \dim_{\mathbb{F}_q} C - 2c.$$

Summarizing these observations, we have the following theorem. Notice that a close result has been given in [15] for binary codes.

Theorem 7 *Let $C \subseteq \mathbb{F}_q^{2n}$ be an $\mathbb{F}_q$-linear code with $\dim_{\mathbb{F}_q} C = n - k$ and $C \subseteq C^{\perp_s}$. Assume that a positive integer c satisfies $2c \leq d_H(C\backslash\{\mathbf{0}\}) - 1$; then, the punctured code $P(C)$ provides an*

$$[[n - c, k + c, \geq d_s(C^{\perp_s}\backslash C); c]]_q$$

entanglement-assisted code.

Our next two sections are devoted to give similar results but considering Hermitian or Euclidean inner product.

4.2 Hermitian inner product

Let $C \subseteq \mathbb{F}_{q^2}^n$ be an $\mathbb{F}_q$-linear code. The *h-puncturing* of C to the coordinate set $\{1, 2, \ldots, n - c\}$ is the code of length $n - c$ defined as

$$P_h(C) = \left\{(a_1, a_2, \ldots, a_{n-c}) \mid (a_1, a_2, \ldots, a_n) \in C \text{ for some } a_{n-c+1}, \ldots, a_n \in \mathbb{F}_{q^2}\right\}.$$

The *h-shortening* of C to the coordinate set $\{1, 2, \ldots, n - c\}$ is the code of length $n - c$ defined as

$$S_h(C) = \{(a_1, a_2, \ldots, a_{n-c}) \mid (a_1, a_2, \ldots, a_{n-c}, 0, \ldots, 0) \in C\}.$$

The above concepts allow us to state the following theorem.

Theorem 8 *Let $C \subseteq \mathbb{F}_{q^2}^n$ be an $\mathbb{F}_{q^2}$-linear code with $\dim_{\mathbb{F}_{q^2}} C = (n - k)/2$ and suppose that $C \subseteq C^{\perp_h}$. Let c be a positive integer such that $c \leq d_H(C\backslash\{\mathbf{0}\}) - 1$, then the punctured code $P_h(C)$ provides an*

$$[[n - c, k + c, \geq d_H(C^{\perp_h}\backslash C); c]]_q$$

entanglement-assisted code.

Proof By the assumption, $\dim_{\mathbb{F}_{q^2}} P_h(C) = \dim_{\mathbb{F}_{q^2}} C$. By a similar argument to that used in Sect. 4.1, we also see that $P_h(C) \cap P_h(C)^{\perp_h} = S_h(C)$. Now we have that $c \leq d_H(C\backslash\{\mathbf{0}\}) - 1$, so $\dim_{\mathbb{F}_{q^2}} P_h(C) = \dim_{\mathbb{F}_{q^2}} C$ and $\dim_{\mathbb{F}_{q^2}} S_h(C) = \dim_{\mathbb{F}_{q^2}} C - c$ [20]. It also holds that $d_H(P_h(C)^{\perp_h}\backslash S_h(C)) \geq d_H(C^{\perp_h}\backslash C)$, and this concludes the proof by Theorem 3. □

4.3 Euclidean inner product

Our result concerning Euclidean duality is the following:

Theorem 9 *Let $C_2 \subseteq C_1 \subseteq \mathbb{F}_q^n$ be two $\mathbb{F}_q$-linear codes such that $\dim C_i = k_i$, $1 \leq i \leq 2$. The standard construction of CSS codes uses $C_2 \times C_1^{\perp}$ as the stabilizer. Assume that c is a positive integer such that*

$$c \leq \min\left\{d_H(C_2 \backslash \{\mathbf{0}\}), d_H(C_1^{\perp} \backslash \{0\})\right\} - 1,$$

then the punctured code $P_h(C_2) \times P_h(C_1^{\perp})$ provides an

$$[[n-c, k_1 - k_2 + c, \geq \min\left\{d_H(C_1 \backslash C_2), d_H(C_2^{\perp} \backslash C_1^{\perp})\right\}; c]]_q$$

entanglement-assisted code.

Proof The assumption $c \leq \min\{d_H(C_2\backslash\{\mathbf{0}\}), d_H(C_1^{\perp}\backslash\{0\})\} - 1$ implies the following two equalities: $\dim_{\mathbb{F}_q} P_h(C_2) = \dim_{\mathbb{F}_q} C_2$ and $\dim_{\mathbb{F}_q} P_h(C_1^{\perp}) = \dim_{\mathbb{F}_q} C_1^{\perp}$. Therefore,

$$\dim_{\mathbb{F}_q} P(C_2 \times C_1^{\perp}) = \dim_{\mathbb{F}_q} P_h(C_2) + \dim_{\mathbb{F}_q} P_h(C_1^{\perp}) = n - (k_1 - k_2).$$

Furthermore, it holds that

$$\begin{aligned}
&\dim_{\mathbb{F}_q} P(C_2 \times C_1^{\perp}) \cap P(C_2 \times C_1^{\perp})^{\perp_s} = \dim_{\mathbb{F}_q} S(C_2 \times C_1^{\perp}) \\
&= \dim_{\mathbb{F}_q} [S_h(C_2) \times S_h(C_1^{\perp})] = \dim_{\mathbb{F}_q} S_h(C_2) + \dim_{\mathbb{F}_q} S_h(C_1^{\perp}) \\
&= \left(\dim_{\mathbb{F}_q} S_h(C_2) - c\right) + \left(\dim_{\mathbb{F}_q} S_h(C_1^{\perp})\right) = n - (k_1 - k_2) - 2c.
\end{aligned}$$

Applying Theorem 7 to the code $C_2 \times C_1^{\perp}$, the proof is completed. □

Acknowledgements We thank Francisco R. Fernandes and Ruud Pellikaan for pointing out a mistake in Theorem 6 on an earlier version of this article.

References

1. Aschbacher, M.: Finite Group Theory, Cambridge Studies in Advanced Mathematics, vol. 10, 2nd edn. Cambridge University Press, Cambridge (2000)
2. Ashikhmin, A., Knill, E.: Nonbinary quantum stabilizer codes. IEEE Trans. Inf. Theory **47**(7), 3065–3072 (2001)
3. Brun, T., Dvetak, I., Hsieh, M.H.: Correcting quantum codes with entanglement. Science **314**(5798), 436–439 (2006)
4. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction and orthogonal geometry. Phys. Rev. Lett. **78**(3), 405–408 (1997)
5. Calderbank, A.R., Rains, E.M., Shor, P.W., Sloane, N.J.A.: Quantum error correction via codes over GF(4). IEEE Trans. Inf. Theory **44**(4), 1369–1387 (1998)

6. Chen, X., et al.: Entanglement-assisted quantum MDS codes constructed from negacyclic codes. Quantum Inf. Process. **16**, 303 (2017)
7. Galindo, C., Hernando, F., Ruano, D.: Stabilizer quantum codes from J-affine variety codes and a new Steane-like enlargement. Quantum Inf. Process. **14**, 3211–3231 (2015)
8. Galindo, C., Geil, O., Hernando, F., Ruano, D.: New binary and ternary LCD codes. IEEE Trans. Inf. Theory **65**(2), 1008–1016 (2019)
9. Guenda, K., Jitman, S., Gulliver, T.A.: Constructions of good entanglement-assisted quantum error correcting codes. Des. Codes Cryptogr. **86**, 121–136 (2018)
10. Gottesman, D.: A class of quantum error-correcting codes saturating the quantum Hamming bound. Phys. Rev. A **54**, 1862–1868 (1996)
11. Grove, L.C.: Classical Groups and Geometric Algebra, Graduate Studies in Mathematics, vol. 39. American Mathematical Society, Providence (2002)
12. Hsieh, M.H., Dvetak, I., Brun, T.: General entanglement-assisted quantum error-correcting codes. Phys. Rev. A **76**, 062313 (2007)
13. Ketkar, A., Klappenecker, A., Kumar, S., Sarvepalli, P.K.: Nonbinary stabilizer codes over finite fields. IEEE Trans. Inf. Theory **52**, 4892–4924 (2006)
14. La Guardia, G.G.: On the construction of nonbinary quantum BCH codes. IEEE Trans. Inf. Theory **60**, 1528–1535 (2014)
15. Lai, C.-Y., Brun, T.A.: Entanglement-assisted quantum error-correcting codes with imperfect ebits. Phys. Rev. A **86**, 032319 (2012)
16. Lai, C.-Y., Brun, T.A., Wilde, M.M.: Dualities and identities for entanglement-assisted quantum codes. Quantum Inf. Process. **13**, 957–990 (2014)
17. Liu, Y., Li, R., Lv, L., Ma, Y.: Application of constacyclic codes to entanglement-assisted quantum maximum distance separable codes. Quantum Inf. Process. **17**, 210 (2018)
18. Luo, L., Ma, Z., Wei, Z., Leng, R.: Non-binary entanglement-assisted quantum stabilizer codes. Sci. China Inf. Sci. **60**, 42501 (2017)
19. Matsumoto, R., Uyematsu, T.: Lower bound for the quantum capacity of a discrete memoryless quantum channel. J. Math. Phys. **43**(9), 4391–4403 (2002)
20. Pless, V.S., Huffman, W.C., Brualdi, R.A.: An introduction to algebraic codes. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, pp. 3–139. Elsevier, Amsterdam (1998)
21. Qian, J., Zhang, L.: On MDS linear complementary dual codes and entanglement-assisted quantum codes. Des. Codes Cryptogr. **87**, 1565–1572 (2018)
22. Ruano, D.: The metric structure of linear codes. In: Singularities, Algebraic Geometry, Commutative Algebra, and Related Topics, pp. 537–561. Springer, Berlin (2018)
23. Seroussi, G., Lempel, A.: Factorization of symmetric matrices and trace-orthogonal bases in finite fields. SIAM J. Comput. **9**, 758–767 (1980)
24. Shor, P.W.: Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A **52**, 2493–2496 (1995)
25. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, pp. 124–134 (1994)
26. Wilde, M.M., Brun, T.A.: Optimal entanglement formulas for entanglement-assisted quantum coding. Phys. Rev. A **77**, 064302 (2008)